

What is claimed is:

SUB A57

1. A method, comprising:

storing encrypted information associated with a computer program;

obtaining personal information as part of a startup sequence for said computer program; and

reading said encrypted information, decrypting information contained therein to obtain decrypted information, and comparing said personal information with said decrypted information; and allowing said computer program to run normally only if said personal information agrees with said decrypted information in a specified way.

2. A method as in claim 1, wherein said personal information is biometric information, and said comparing comprises comparing said biometric information with other biometric information in said encrypted information

3. A method as in claim 2, further comprising installing said computer program by entering a biometric code, sending said biometric code to a server, encrypting said biometric code at

4 said server and returning an encrypted sequence to said software
5 as said encrypted information.

1 4. A method as in claim 3, wherein said encrypting uses a
2 private key at said server, and said decrypting verifies a
3 signature of said private key.

1 5. A method as in claim 3, wherein said encrypting uses a
2 private key at said server, and said decrypting uses a public
3 key included as a part of said computer program.

1 6. A method as in claim 1, further comprising determining
2 if a biometric reader is attached to a port, and wherein said
3 program is only allowed to run if said biometric reader is
4 attached to said port.

1 7. A method as in claim 1, further comprising allowing the
2 software to run in a limited exception mode without establishing
3 that said personal information agrees with said decrypted
4 information.

1 8. A method, comprising:
2 requesting a computer system to install a specified
3 computer program;

4 determining whether said computer program is verified for
5 installation;

6 obtaining a reference biometric information from the
7 authorized user; and

8 thereafter allowing said program to run normally only when
9 biometric information is obtained which matches said reference
10 biometric information.

1 9. A method as in claim 8 wherein said determining
2 comprises determining if the specified license has already been
3 used for another installation.

1 10. A method as in claim 8 wherein said determining uses a
2 specified unique code that was distributed with the program, and
3 determines from a server whether said unique code has already
4 been used for an installation.

1 11. A method as in claim 8, further comprising, after
2 determining that said installation is authorized, sending said
3 reference biometric information to a server.

1 12. A method as in claim 11, further comprising, at the
2 server, encrypting said reference biometric information, and

3 returning encrypted biometric reference information which is
4 stored with said program, and which is used by said allowing.

1 13. A method as in claim 8, wherein said allowing
2 retrieves encrypted biometric information, decrypts said
3 biometric information, and allows said program to run normally
4 only if said decrypted biometric information matches a currently
5 entered biometric information.

1 14. A method as in claim 12, wherein said reference
2 biometric information is encrypted at said server using a
3 private key of a public key-private key pair, and said reference
4 biometric information is decrypted when software is to be run,
5 using said public key corresponding to said private key.

1 15. A system, comprising:
2 in a computer, run an operating system, which includes an
3 ability to run an associated program;
4 at least one port, associated with said computer, said port
5 capable of receiving at least one vertebral device thereon; and
6 a user interface, associated with said computer, receiving
7 a command to run a specified program, and operating to decrypt
8 reference biometric information associated with said specified
9 program, compare currently-obtained biometric information with

09712358-11400

10 said reference biometric information, and allows said program to
 11 run in a specified way only when said currently-obtained
 12 biometric information matches said reference biometric
 13 information.

1 16. A system as in claim 15, wherein said operating system
 2 operates to first detect whether a biometric reading device is
 3 attached to said port, and then detect whether biometric
 4 information has been received from said biometric reading
 5 device, said program being allowed to run in said specified way
 6 only when both said biometric reading device is attached, and
 7 biometric information which is received matches said reference
 8 biometric information.

1 17. A system as in claim 15, wherein said operating system
 2 decrypts said reference biometric information.

1 18. A system as in claim 17, wherein said operating system
 2 determines a time and current biometric information is obtained,
 3 and compares said time with the current time, and allows said
 4 program to run in in said specified way only when said time is
 5 within a specified interval of said current time.

1 19. A computer readable media, containing instructions
2 causing the computer to:
3 detect a request to run a specified program;
4 obtain current biometric information;
5 decrypt an encrypted reference information including
6 reference biometric information therein, and obtaining reference
7 biometric information therefrom;
8 compares said reference biometric information with said
9 current biometric information; and
10 allow said specified program to run into specified way only
11 when said reference biometric information matches said current
12 biometric information.

1 20. Instructions as in claim 19, wherein said compares
2 also compares a time and current biometric information was
3 obtained with a current time, and allows said specified program
4 to run in the specified way only man said time is within a
5 specified interval of said current time.

1 21. Instructions as in claim 19, wherein the specified way
2 is an unrestricted run which does not detect a number of other
3 executions or operations of said program.

09712398.11400